Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.235

X-box를 이용한 Session-oriented Cross play에 대한 보안 요구사항 분석*

김 동 우,† 강 수 영, 김 승 주‡
고려대학교 정보보호대학원

Analysis of Security Requirements for Session-Oriented Cross Play Using X-box*

Dong-woo Kim,† Soo-young Kang, Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

최근 기술의 발달과 산업의 변화를 통해 게임업계는 PC와 Mobile 그리고 Console game에서 서로 다른 플랫폼 유저가 함께 즐길 수 있는 크로스플레이를 지원하여 재미를 극대화 하고 있다. 크로스플레이를 통해 플랫폼의 경계가 없어지면 기존의 보안이 일정수준 이상 유지되었더라도 새로운 서비스로 인해 예상치 못한 보안위협이 발생 할 수 있다. 기존에 진행된 온라인 게임보안 연구는 PC와 Mobile환경에서 발생 가능한 부정행위 탐지가 대부분이지만 크로스플레이가 가능해짐에 따라 Console game에 대한 보안연구 역시 필요하다. 따라서 본 논문은 Console game 유저를 대상으로 크로스플레이를 즐길 때 발생 가능한 보안위협을 STRIDE와 LINDDUN 위협모델링을 활용하여 체계적으로 식별하고 국제공통평가기준을 활용해 보안요구사항 도출하여 크로스플레이에 대한 평가 기준을 제시한다.

ABSTRACT

Recent technological advances and industry changes, the game industry is maximizing fun by supporting cross-play that can be enjoyed by different platform users in PC, Mobile and Console games. If the boundaries are lost through the cross play, unexpected security threats can occur due to new services, even if existing security is maintained above a certain level. The existing online game security researches are mostly fraud detection that can occur in PC and mobile environment, but it is also necessary to study the security of the console game as cross play becomes possible. Therefore, this paper systematically identifies the security threats that can occur when enjoying cross play against console game users using STRIDE and LINDDUN threat modeling, derives security requirements using the international common evaluation standard.
Keywords: Threat Modeling, STRIDE, LINDDUN, Security requirements, Cross-play, Console game

I. 서 론

온라인게임은 가장 성공적인 인터넷 서비스로 다양하고 극적인 재미를 통해 지속적으로 성장하고 있다. Newzoo 사의 2017년 보고서에 의하면[1] 글로벌 게임시장의 매출은 지난해 대비 10.7% 상승한

Received(11. 26. 2018), Modified(01. 07. 2019), Accepted(01. 07. 2019)
* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음(과제번호 H2101-18-1001)
† 주저자, mecomto@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

약 125조 원을 기록 했고 콘솔게임은 약 35조 원 매출을 올리며 3.7%의 성장세를 보였다. 스마트폰의 폭발적인 보급과 간편한 접근성으로 모바일게임의 성장이 가장 높지만 아시아권과 달리 북미와 유럽에서는 Fig. 1과 같이 콘솔게임의 점유율이 여전히 강세를 보였다. 지금까지 콘솔게임 시장에 소극적인 자세를 보였던 국내 대형 게임사들도 지역 간 플랫폼 선호 유형을 고려하여 각 게임사의 대표 인기 지적재산권(IP)을 활용해 콘솔게임시장의 진출을 가속화하고 있다[2]. 이처럼 하나의 게임 콘텐츠가 특정 플랫폼에 국한되지 않고 여러 플랫폼에서 동시에 즐기면서 크로스플레이가 가능하게 되었다. 즉 유무선 네트워크를 통해 하나의 게임을 여러 플랫폼의 유저가 함께 플레이 할 수 있게 되었다. 하지만 크로스플랫폼 게임을 서비스하기 위한 체계적인 개발 기술과 기획이 미흡한 단계에 있다. 실제로 현재까지 크로스플레이를 지원하는 대부분의 게임은 특정 플랫폼에서 서비스된 후 타 플랫폼으로 전환되어 재출시 된다. 이런 경우 게임기획 단계부터 체계적으로 제작되지 않고 플랫폼별 입출력방식, 오디오와 비디오에 따른 코덱의 차이만 고려하여 개발한다. 또한 인터페이스 차이로 인한 로드밸런싱 문제, 성능에 따른 그래픽 처리 시간, 디스플레이 렌더링과 같이 게임에 필요한 요소는 클라우드 서비스 제공 기업과 게임엔진에만 의존하고 있다. 이처럼 게임회사는 개발 작업을 간소화하여 게임시장의 급격한 성장과 트렌드의 변화 속도를 맞추지만 보안에 대한 반영은 미흡한 실정이다. 단독 플랫폼에서 실행되는 게임보다 많은 부분을 고려해야 하는 크로스플레이 서비스는 외부 계정과의 연동 및 다수의 데이터 처리에 따른 예상하지 못한 보안위협이 발생 할 수 있다. 새로운 서비스를 통해 계정이 탈취되면 게임내 재화에 심각한 손해를 보고 관련된 개인정보 역시 노출될 가능성이 크다. 또한 개조한 펌웨어와 변조된 파일을 통해 인가되지 않은 매크로 프로그램을 구동할 수 있게 된다. 따라서 본 논문은 크로스플레이에서 발생할 수 있는 잠재적 위협을 기존에 연구되지 않은 콘솔기기를 대상으로 분석 한다. 본 논문은 다음과 같이 구성된다. 2장에서는 보안위협모델링 및 콘솔게임 관련연구를 소개하고 3장에서는 위협 모델링 기법을 활용해 위협을 도출한다. 4장에서는 국제공통평가기준을 통해 보안요구사항을 도출하고 마지막으로 5장에서는 본 논문의 결론 및 향후 연구 방향을 제시 한다.

II. 관련 연구

2.1 보안 위협 모델링

위협모델링은 분석범위를 식별하고 소프트웨어, 시스템 또는 특정 서비스에 대해 발생 할 수 있는 잠재적 위협을 도출한 뒤 우선순위를 부여하는 구조화된 접근 방법이다. 위협모델링 종류에는 크게 상업적 제품과 표준방식이 있다. 상업적 제품에는 설계단계부터 다양한 위협을 식별할 수 있는 Microsoft의 STRIDE[3]와 공식적인 소프트웨어 방법을 평가하고 보안 수준을 결정하기 위한 SUN의 ACSM/SAR[4]가 있다. 표준에는 NIST의 정보시스템에 대한 자동 보안평가도구인 ASSET[5], 조직 위험관리에 대해 운영상의 위협 및 취약성을 평가하는 OCTAVE[6], 조직의 컴플라이언스 및 비즈니스 분석을 고려한 PASTA[7], 감사 프로세스를 충족시키는 Trike가 있다[8]. 그리고 개인정보에 대한 위협모델링 종류에는 본 논문에서 활용한 LINDDUN[9]와 프라이버시를 식별하고 위협을 완화하기 위해 목표를 도출하는 PIA[10], 거래나 매매 중 노출된 관계자 신원에 관한 정보의 양을 측정하는 Nymity[11] 등이 있다.

2.1.1 STRIDE 위협 모델

STRIDE는 Microsoft사의 보안전문가인 Loren Kohnfelder와 Praerit Gard가 개발한 보안위협모

Table 1. STRIDE Security Property Description

Threat	Description
Spoofing	Unauthorized entity is disguised as authorized entity
Tampering	Threats to tamper with information
Repudiation	Threats to tamper with components
Information Disclosure	Critical data is exposed
Denial of Service	Behavior such as resource consumption prevents normal operation
Elevation of Privilege	Execute with high privileges for subjects without access and execution rights

델링 방법으로 분석시스템의 공격유형을 정의하기 위해 설계하였다. 이를 활용하면 분석자의 역량에 따른 영향을 최소화 할 수 있는 장점이 있다. STRIDE는 보안의 3요소 기밀성(confidentiality), 무결성(integrity), 가용성(availability)에 부인방지(non-repudiation), 인증(authentication), 권한부여(authorization)를 합한 총 6가지의 보안속성에 반대되는 위협들의 약어를 의미한다. Table 1은 위협에 상응하는 속성과 정의를 나타낸 표이다.

2.1.2 LINDDUN 위협 모델

LINDDUN은 벨기에 루벤의 가톨릭 대학에서 개발된 방법론으로 개인정보 문제를 체계적으로 고려하도록 권장하는 위협모델링 기술이다. LINDDUN의 각 약어는 연결 가능성(linkability), 식별성(identifiability), 부인 방지(non-repudiation), 검출능력(detectability), 정보노출(disclosure of information), 내용 비인식(unawareness), 정책 동의 불이행(non-compliance) 앞 글자를 의미 한다. Table 2는 각 요소에 대한 정의를 나타낸 표이다.

Table 2. LINDDUN Security Property Description

Threat	Description
Linkability	Not being able to hide the link between two or more identities of information
Identifiability	Being able to sufficiently identify the subject within a set of subjects
Non-repudiation	Not being able to deny a claim
Detectability	Being able to sufficiently distinguish whether an item of interest exists or not
Disclosure of information	Critical data is exposed
Unawareness	unaware of the consequences of sharing information.
Non-compliance	Not being compliant with legislation, regulations, and corporate policies.

Table 3. Components of Data Flow Diagram

Element	Symbol	Description
External Entity	□	Code outside Control
Process	○	Any running Code
Data Store	=	Things that store data
Data Flow	→	Communication between process
Trust Boundary	⬚	Anyplace where various principles come together

2.2 콘솔 게임 연구 및 보안위협

2.2.1 콘솔게임 관련 연구

패드와 눈으로만 즐기는 게임에서 몸을 이용한 모션 캡처와 음성 인식이 가능한 신규 게임의 등장으로 콘솔 게임에 대한 연구가 활발히 진행되고 있다.

Johnny Chung은 [12]에서 닌텐도 Wii 리모컨의 기술 및 내부 동작과정에 대해 언급하고 다양한 I/O기능을 통해 장치의 추가 활용 용도에 대해 언급하였다.

Arunasalam은 [13]에서 Microsoft의 주변기기 Kinect에서 사용된 기술이 가상현실, 움직임 추적 등 효과적으로 인공지능에 활용 가능하지만 움직임 응답에 대한 해킹으로 사용자의 개인정보가 침해될 수 있다고 결론을 맺었다.

Jeff Yan 외 1명은 [14]에서 온라인 게임의 알려진 다양한 부정행위에 대해 요약하고 보안전문가와 게임 개발자에게 도움이 되는 게임 부정행위 분류법에 대해 정의하였다. 특히 온라인 게임 및 콘솔 게임에서 발생 할 수 있는 취약점을 설계, 구현, 개발 단계에서 발생 할 수 있는 결함으로 분류하였다.

Jason Moore 외 3명은 [15]에서 Microsoft Xbox를 포렌식 관점에서 연구하였다. MFT (Master File Table)에서 발견된 메타 데이터를 통해 응용 프로그램을 사용한 시간과 시스템 복원에 관한 분석을 진행 하였다.

2.2.2 콘솔게임 보안위협

본 장에서는 콘솔게임을 대상으로 클라이언트, 네트워크에서 발생되었던 보안위협을 분석한다. 대부분 콘솔게임 보안 사고는 저장매체의 기술적 보호 조치

를 무력화 하는 형태의 해킹 및 펌웨어 개조로 발생하였다. 게임기 세대에 따라 콘솔 저장매체는 카트리지, 광디스크와 같은 물리적 패키지로 현재는 디지털 다운로드 방식과 병행하여 서비스를 제공한다. 카트리지는 단단한 케이스로 파손의 위험이 적고 복제가 쉽지 않은 매체이지만 Multicart를 통해 여러 가지 게임을 하나의 카트리지에서 즐기면서 정품 카트리지를 구매하지 않고 게임을 플레이 하였다. 이후 새로운 저장매체인 CD-ROM으로 교체했고 게임사는 게임기내에 정품여부를 구분하는 Boot-Rom기술을 탑재하여 불법복제 매체를 인식하지 못하도록 하였다. 하지만 공격자들은 별도의 회로로 구성된 작은 기판인 모드칩을 게임기 본체 메인보드에 장착해 Access Code역할을 대체하여 정품 인식 기능을 무력화하였다. 이후 Sega는 기존의 CD-ROM형식이 아닌 GD-ROM을 통해 모드칩의 사용을 차단하였으나 Utopia Boot Disc를 통해 불법복제 게임 데이터를 실행 하였고 닌텐도 DS역시 기존의 카트리지보다 작은 크기의 저장매체를 배포를 하였는데 R4 및 DSTT와 같은 메모리 리더기를 통해 우회하여 사용하였다. 가장 최근 발매된 닌텐도 스위치 역시 Plutoo 외 2명의 해커들에 의해 취약점이 발견되었다. 이들은 34C3 해킹학회에서 닌텐도 스위치에 탑재된 커널에 대한 임의적 권한을 획득한 결과물을 소개했다. 스위치 내부에 탑재된 NVIDIA Tegra X1의 CPU가 Out-of-Order Execution와 Speculative execution을 사용하는 Cortex-A57에 기반하고 있기 때문에 멜트다운 및 스펙터 취약점이 존재한다고 발표하였다. 콘솔게임의 공격은 대부분 펌웨어 및 하드웨어 개조를 통해 불법복제 게임을 즐기는 형태로 온라인게임과 모바일게임에 비해 쉽지는 않지만 원본 게임에서 수정된 부분만을 배포하는 식으로 공유가 활발히 되고 있다. 또한 게임 내 함수 변조 및 후킹으로 장애물 뒤의 적을 볼 수 있는 Wallhack, 좌표를 계산하여 자동으로 적군을 조준해주는 Aimbot, 그리고 적군에게 공격을 당해도 체력이 줄지 않는 Infinite health등 온라인과 모바일게임에서 존재하는 다양한 게임불법 프로그램도 콘솔게임에 존재한다.

III. 크로스플레이 보안 위협 식별

3.1 가정 사항

본 논문에서는 명확한 데이터 흐름을 파악하기 위해 분석범위를 다음과 같이 가정한다. 크로스플레이를 지원하는 게임 중 매치메이킹을 통해 모든 플레이어가 동시에 게임에 참여하는 Session-oriented형태의 실시간 멀티 플레이 게임을 분석한다. 클라이언트는 Serverless Computing의 인스턴스에 개발된 Dedicated Server와 통신하고 계정 연동에 필요한 서비스는 웹 브라우저를 통해 그리고 게임 클라이언트는 Xbox-One에서 실행 한다고 가정한다. 각 데이터 흐름에 대한 자세한 내용은 3.2.1절에서 설명한다.

3.2 Data Flow Diagram을 이용한 분석

DFD는 위협 모델링의 첫 번째 단계로 분석 시스템의 데이터 흐름을 가시적으로 파악하여 분석범위를 식별하기 위해 Table 3의 총 5가지 요소를 활용하여 작성한다. 본 논문은 Microsoft Threat Modeling Tool2016을 사용하여 크로스플레이에 대한 데이터 흐름을 Fig. 2와 같이 총 6개의 외부 객체, 11개의 프로세스, 2개의 저장소 그리고 6개의 경계를 도출하였다.

3.2.1 크로스플레이 데이터 흐름 파악

(1) Console User Boundary to Game Authentication Boundary

콘솔유저가 게임구매, 멀티플레이를 즐기기 위해서는 콘솔게임 제조사에서 제공하는 네트워크 계정이 필요하다. 해당 구간은 OAuth2.0 토큰 기반 인증 시스템을 사용해 콘솔 네트워크 계정과 게임계정 연동을 나타내었다.

세션 기반 인증과 달리 토큰 기반 인증은 로그인 정보를 다른 서비스에 공유함으로서 다양한 디바이스를 호환 할 수 있는 장점이 있다. 최초로 사용자(E1)가 게임 서비스에 가입요청을 하면 게임 웹 서버(E2)는 플랫폼 선택(P7)을 통해 사용자가 플레이할 콘솔게임 네트워크 계정 인증 서버로 URL redirection한다. 이후 콘솔 인증 서버는 로그인창을 통해 유저를 인증하고 엑세스 토큰과 교환할 수

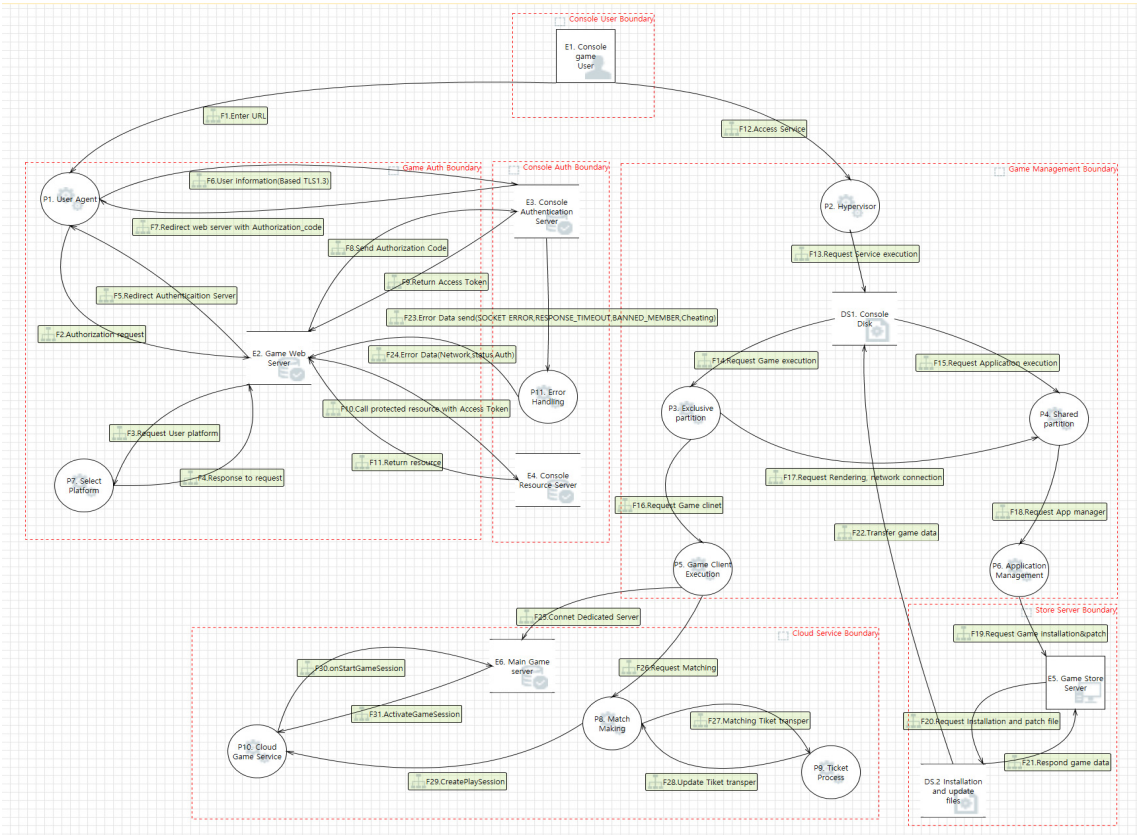

Fig. 2. Level2 DFD for Cross-play platform Service

있는 인가코드를 게임 웹 서버에 제공한다. 게임 웹 서버는 저장된 인가코드를 다시 토큰 엔드 포인트로 교환 요청을 시도하고 콘솔 인증 서버는 인가코드의 유효성을 검증하여 엑세스 토큰을 전송해 준다. 해당 토큰을 사용하여 콘솔 자원서버(E4)에 접근하여 콘솔 사용자 프로파일과 계정정보를 게임계정과 연동한다.

(2) Comprehensive Boundary to Error Handling Process

게임계정인증, 계정연동, 게임실행, 메인게임서버 등 모든 구간에서 발생 할 수 있는 오류를 재시작(P11)로 처리하는 데이터 이동구간이다. 게임데이터가 예정대로 전달되지 않거나 회선상의 문제로 인한 네트워크 오류, 유효하지 않는 회원, 적절하지 않은 토큰정보, 게임클라이언트의 상태 그리고 외부 인증 라이브러리 오류 등이 존재한다. 구간별 오류처리는 Table 4를 통해 설명한다.

(3) Game Management to Store Server Boundary

콘솔장비에서 DLC(Download Contents)를 사용하여 Game Store Server(P4)로 부터 게임 데이터를 전달받는 구간이다. 콘솔장비를 실행하면 하드웨어 자원을 관리하는 Host OS가 Hyper-v(P2)프로세스에 의해 실행된다. 해당 프로세스는 가상 머신 기술로 게임에 필요한 서비스 제공은 Shared OS(P4)로 게임플레이는 Exclusive OS(P3)에서 실행 하도록 분리하여 서로 안전한 상태를 유지 하고 하드웨어의 변경에도 게임의 호환성을 유지하기 위해 사용한다. 이후 부팅된 Shared OS에 의해 사용자는 게임 설치 및 패치를 Game Store에 요청하고 콘솔장비 내부에 있는 저장장치로 게임 데이터를 전송 받는다.

(4) Game Management to Game Server Boundary

게임클라이언트 실행 이후 사용자 매칭 및 서버내부 데이터 이동 구간이다. 크로스플랫폼은 다양한 플

Table 4. Error Handling Process

Category	Error	Explanation
Authentication & SP_Authentication	Invalid_User	Request for an invalid member.
	User_Canceled	Login has been canceled.
	Not_exist_User	Member who does not exist or has left.
	Access Token Failed	Token login failed.
	Not_Invalid_Token	Token information is not valid.
	Invalid_IdP_Info	IdP information is not valid.
	Access code expire	The access code has expired.
Game Management	Guest access_Failed	Information of the terminal accessing should be deleted.
	Socket_error	Function of the network socket is not normal.
	Response_timeout	Response time has been exceeded.
	GameClient_State Code Error	Game client's status information does not match the normal code.
	Ban_Member	Account has been suspended due to fraud.
	Not_Playable	Can not be played due to a check or patch.
	Unknown_error	Unknown error occurs.

랫폼과 유무선 네트워크를 통해 연동되기 때문에 사용자들의 게임 환경, 네트워크의 전송 속도, 지연 시간, 그래픽 성능차이를 실시간으로 처리해야 한다. 이와 같은 성능 이슈를 해결하기 위해 Serverless Computing 서비스에서 제공하는 SDK를 사용하여 Dedicated Server를 개발하고 클라우드에서 운영하는 방식으로 게임 서비스를 제공한다. 콘솔게임 사용자는 게임실행 후 타 플랫폼 사용자를 초대하고 사전에 정의된 규칙을 사용해 효율적인 매치를 제공하는 Match Making 프로세스(P8)를 통해 적합한 플레이어를 검색한다. 이후 매칭 가능한 그룹을 생성하고(P9) 새로운 게임 세션을 생성하는 함수를 Cloud Game Service(P10)에 요청한 후 생성된 게임세션을 통해 실시간 멀티 플레이를 즐길 수 있다.

3.3 Attack Library 수집 및 구축

Attack Library는 분석시스템에 대한 위협들을 다양한 자료를 통해 수집한 목록을 말한다. STRIDE와 LINDDUN을 이용해 3.2장에서 파악한 DFD를 바로 분석하면 추상적인 위협만을 식별하기 때문에 논문, 표준, 기술보고서, CVE의 공개된 취약점, 그리고 권위 있는 보안컨퍼런스 발표 등의 자료를 활용하여 근거를 제시한다. 다음 Table 5는 위의 자료들을 참고하여 조사한 Attack Library이다.

Table 5. Attack Library for Cross-play

Type	Category	Topic	No	Source	Title	Ref
Paper	Access	Physical Access	1	IEEE	Social Engineering Attack Framework	[16]
		Authentication	2	IEEE	Understanding cloud computing vulnerabilities	[17]
			3	Elsevier	A survey of intrusion detection techniques in cloud	[18]
		Omitted				
	Network	Cloud Service	7	IEEE	Network security for virtual machine in cloud computing	[19]
			8	IJETER	A Survey of Security Issues and Attacks in Cloud and their Possible Defenses	[20]
			9	Computers &	Building safe PaaS clouds: A survey on security in multi tenant software	[21]

Type	Category	Topic	No	Source	Title	Ref
				Security	platforms	
		Omitted				
		Game Cheating	12	IEEE	An Investigation of Cheating in Online Games	[22]
			13	IJCSIT	IT security issues within the video game industry	[23]
	Internet Service	Protocol	14	IEEE	Splitting the HTTPS stream to attack secure web connections	[24]
			15	WWW '08	Force HTTPS: protecting high-security web sites from network attacks	[25]
		Omitted				
		Web Service	18	IEEE	Security vulnerabilities in modern web browser architecture	[26]
			19	ACM	XML signature element wrapping attacks and countermeasures.	[27]
			20	IEEE	Automatic creation of SQL injection and cross-site scripting attacks	[28]
		Availability	21	Elsevier	Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks	[29]
			22	IGI	DoS Attacks Over Cloud Environment: A Literature Survey	[30]
		Omitted				
	Storage	Data Loss	25	IEEE	Security and privacy in cloud computing	[31]
			26	CCPE	An overview of insider attacks in cloud computing.	[32]
		Omitted				
	Hardware	GPU	29	IEEE	Stealing web pages rendered on your browser by exploiting GPU vulnerabilities	[33]
			30	ETS	Vulnerable GPU memory management: towards recovering raw data from GPU	[34]
		Omitted				
		virtualization	33	IJICT	Hypervisor Security - A Major Concern	[35]
			34	CSUR	A survey of security issues in hardware virtualization	[36]
		system	35	IEEE	Embedded systems security: Threats, vulnerabilities, and attack taxonomy	[37]
			36	NDSS	When Firmware Modifications Attack: A Case Study of Embedded exploitation	[38]
			37	IEEE	A Methodology for Forensic Analysis of Embedded Systems	[39]
Conference	Access	Authentication	38	2016ACM SIGSAC	A Comprehensive Formal Security Analysis of OAuth 2.0	[40]
			39	SAFECOMP 2017	Security Flows in OAuth 2.0 Framework: A Case Study	[41]
			40	RSA Conference	Leaking Ads—Is User Data Truly Secure?	[42]

Type	Category	Topic	No	Source	Title	Ref
	Internet Service	Protocol	41	2009 BlackHat	New tricks for defeating SSL in practice.	[43]
		Availability	42	CCSW`10	A new form of DoS attack in a cloud and its avoidance mechanism	[44]
	Hardware	virtualization	43	IEEE Conference	Network security for virtual machine in cloud computing.	[45]
			44	Black Hat 2018	A Dive in to Hyper-V Architecture & Vulnerabilities	[46]
			45	Black Hat 2018	Hardening Hyper-V through Offensive Security Research	[47]
Standard	Network	IETF	46	RFC6819	OAuth 2.0 Threat Model and Security Considerations	[48]
CVE	Network	Browser	47	CVE-2018-8491	Remote attackers to execute arbitrary code	[49]
			48	CVE-2018-8470	IE Security Feature Bypass Vulnerability	[50]
			49	CVE-2018-8357	Microsoft Browser Elevation of Privilege Vulnerability	[51]
		Omitted				
		Service	53	CVE-2018-5178	Bbuffer overflow was found during UTF8 to Unicode	[52]
			54	CVE-2018-8493	Windows TCP/IP Information Disclosure Vulnerability	[53]
	Access	Authentication	55	CVE-2018-15121	Validate the state parameter of the OAuth 2.0 and OpenID Connect protocols	[54]
	Hardware	virtualization	56	CVE-2018-0957	Information Disclosure Vulnerability	[55]
			57	CVE-2018-8489	Hyper-V Remote Code Execution Vulnerability	[56]
			58	CVE-2018-8438	Hyper-V Denial of Service Vulnerability	[57]
		Omitted				
	OS	Kernel	62	CVE-2018-8495	Shell Remote Code Execution Vulnerability	[58]
			63	CVE-2018-8492	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability	[59]
Technical Report	Internet Service	Web Service	64	exploit-DB	Microsoft Internet Explorer 11.371.16299.0 (Windows 10) - Denial Of Service	[60]
	Omitted					

3.4 STRIDE를 이용한 분석

STRIDE는 시스템 및 특정서비스의 위협을 추론하고 발견하는데 용이한 위협모델링으로 앞서 분석한 DFD 각 요소의 잠재적인 위협을 식별 할 수 있다. 따라서 해당 절에서는 STRIDE를 활용해 서비스 구간을 집중적으로 분석한다. STRIDE는 DFD의 각 요소별로 적용 가능한 항목에 차이가 있으며 Table 6은 요소별 적용 가능한 STRIDE 항목을 나타내었다. 해당 규칙을 준수해 크로스플레이에 대한

Table 6. Available DFD elements per STRIDE

	S	T	R	I	D	E
Entity	X		X		X	
Data Store		X		X	X	
Process	X	X	X	X	X	X
Data Flow		X		X	X	

Table 7. STRIDE Threat Analysis on Cross play

Element Type	No	Name	STRIDE	Description	Attack Library	Threat
Entity	E1	Console game User	S	Attackers spoofing as other users using social engineering techniques	[1,6,12]	T1
Process	P1	User Agent	S	Spoofing a legitimate web browser	[50,51]	T2
			S	Spoofing a malicious message as a normal message	[19]	T3
			T	Tampering a request message to a game web server	[15]	T4
			T	Remote Code Execution Through Modulated Web Pages	[47,48,52]	T5
			I	Information disclosure by MITM attack	[14,16]	T6
			I	Exposing authentication information through a tampered web page	[18,20]	T7
			D	DoS attack on web server	[21,22,23,24,64]	T8
			E	Get high authority by improperly manipulating messages and browsers	[19,49,53,62]	T9
Process	P2	Hypervisor	I	Obtain user information from Host OS	[34,54,60]	T10
			D	DoS Attacks Due to Inappropriate Privileges Checks in Host OS	[35,58]	T11
			T	Modify device firmware through malware	[36,37,44,45]	T12
			E	Run remote code execution in Host OS	[34,35,57,59]	T13
			E	Elevation of authority through transmitted sessions	[33,35]	T14
Process	P3 & P4	Exclusive partition& Shared partition	T	Change the OS kernel corruption	[63]	T15
			I	Acquisition of data stored in GPU memory	[29,30,32]	T16
			I	Get ciphertext through Side-Channel Attack	[31,32]	T17
			D	DoS attack using GPU via malicious web page	[32,33]	T18
			E	Elevation of privilege through kernel memory	[61,62]	T19
Process	P5	Game Client Execution	T	Modifying Graphics Drivers and Firmware	[12,13]	T20
Process	P6	Application Management	I	Acquisition of data stored in GPU memory	[29,30,32]	T21
			I	Get ciphertext through Side-Channel Attack	[31,32]	T22
			D	DoS attack using GPU via malicious web page	[32,33]	T23
			E	Elevation of privilege through kernel memory	[61,62]	T24
Data Store	DS 1	Console Disk	T	Change file information stored on the console disk via malicious code	[69]	T25
			I	Data Acquisition through BitLocker Bypass	[69]	T26

Element Type	No	Name	STRIDE	Description	Attack Library	Threat
Omitted						
Data Flow	F7	Redirect web server with Authorization_code	T	Obtain user account information with modulated URL Redirect	[38]	T64
			T	Tampering authentication code sent to server	[5,15,17,40,55]	T65
			I	Obtain Client Secret Information through Guessing	[46]	T66
			I	An attacker obtain authorization "codes	[6,16,39,56]	T67
			D	DoS attacks on the server using code	[46]	T68
Data Flow	F8	Send Authorization Code	T	Tampering authentication code sent to server	[5,15,17,40,55]	T69
			T	Tampering normal sites to steal user sessions	[46]	T70
			I	Attacker obtain authorization "codes	[6,16,39,56]	T71
			I	Obtain valid code information through Guessing	[46]	T72
			D	DoS attacks on the server using code	[46]	T73
Data Flow	F9 & F10	Return Access Token & Call protected resource with Access Token	T	Change Access Token	[5,38,55,56]	T74
			T	Obtain user account information with modulated URL Redirect	[46]	T75
			I	Information leak through Access Token eavesdropping	[5,39,46,56]	T76
			I	Obtain Access Token information through browser history	[46]	T77
			I	Obtain a valid Access Token through guessing	[46]	T78

STRIDE분석을 수행한 결과는 Table 7에 나타내었다.

3.5 Attack Tree 작성

STRIDE를 통해 도출된 위협이 실제 공격자가 대상 시스템을 공격하기 위한 방법을 체계화 하고 시각화 하기 위해 Attack Tree를 작성한다. Attack Tree는 공격 유형을 각각의 노드로 표현하고 STRIDE를 통해 발견된 위협들을 하위 노드로 표현한다. Table 8은 앞서 분석한 STRIDE를 바탕으로 Attack Tree를 나타낸 결과이다.

Table 8. Attack Tree for cross-play

Attack Tree				Threats
1	Obtain the account information			
AND	1.1	verification code		
	OR	1.1.1	Man in the middle attack	T4,T6,T46,T49,T56,T65,T69,T74,T76
	OR	1.1.2	SQL Injection	T7,T66,T71
	OR	1.1.3	Session Hijacking	T14,T30,T41,T70,T76
	OR	1.1.4	Insufficient authorization checks	T10,T11,T36,T66,T70
	OR	1.1.5	Redirect Attack	T64,T75
AND	1.2	Client_ID / Secret obtain		
	OR	1.2.1	Authentication information Guessing	T66,T72,T78
	OR	1.2.2	Phishing Attack	T1,T5,T7,T27,T39,T46,T70

Attack Tree					Threats
	OR	1.2.3	Insider Attack		T38,T47,T52,T54,T56,T59
	OR	1.2.4	Spoofing Attack		T1,T2,T28,T34,T40,T46,T61,T70
	OR	1.2.5	Cross-site scripting Attack		T7,T27,T33,T35,T39,T45,T58,T63,T65,T69,T70
	OR	1.2.6	Unsuitable 3rd party policies		T36,T65,T69,T70,T77
	OR	1.2.7	Injection Attack		T3,T77
OR	1.3	Install malicious			
	OR	1.3.1	Malware injection		T38
OR	1.4	Resource Obtain			
	OR	1.4.1	Brute force attack		T8
	OR	1.4.2	Buffer overflow		T9,50,T58,T63
2	Network Attack				
OR	2.1	Function misuse			
	OR	2.1.1	Information exposure		
		OR	2.1.1.1	Backdoor channel attack	T36,T38,T59
Omitted					
3	Server Attack				
OR	3.1		Denial of Service Attack		
	OR	3.1.1	Protocol Attack		
		OR	3.1.1.1	SYN Flooding	T8,T18,T23,T37,T66
		OR	3.1.1.2	Ping of death	T8,T11,T66,T68,T73
		OR	3.1.1.3	HTTP Flooding	T8,T18,T23,T32,T44,T68,T73
	OR	3.1.2	Volume Based Attack		
		OR	3.1.2.1	ICMP Flooding & UDP Flooding	T8,T11,T32,T44,T53,T57,T62,T68,T73
OR	3.2	Leaking confidential Game / User Data			
	OR	3.2.1	Application side		
		OR	3.2.1.1	Firmware tampering	T20,T51,T55,T60
		OR	3.2.1.2	Execute malicious	T31,T38,T43,T51,T52
4	Hardware Attack				
OR	4.1	Hardware tampering			
	OR	4.1.1	Firmware or kernel tampering		T10,T12,T15,T16,T19,T20,T21,T24,T25,T55,T60
Omitted					

3.6 LINDDUN을 이용한 분석

LINDDUN 방법론은 Problem space, Solution space 2개의 공간으로 구성되고 각각은 3개의 단계로 세분화 된다. Problem space는 LINDDUN 모델의 핵심 단계로 분석 시스템의 개인정보 위협을 식별하는 단계이다. 가장먼저 STRIDE모델에서 사용한 DFD를 통해 잠재적 위협을 식별하고 이후 DFD의 각 요소마다 적용 가능한 항목을 Table 9

Table 9. Available DFD elements per LINDDUN

	L	I	N	D	D	U	N
Entity	X	X				X	
Data Store	X	X	X	X	X		X
Process	X	X	X	X	X		X
Data Flow	X	X	X	X	X		X

형태로 비교한다. 마지막으로 Threat Tree를 활용하여 위협이 발생할 수 있는 경우를 나타낸다. Solution space는 식별된 위협을 완화할 수 있는 방법 및 솔루션을 선택하는 단계로 구성된다. 앞서 분석된 위협에 대해 우선순위를 지정하고 LINDDUN 공식 사이트에서 제공하는 완화수단과 개인정보 강화 솔루션을 통해 적합한 해결책을 선택한다. 본 논문에서는 Problem space를 중점적으로 분석하고 분석가마다 다르게 해석할 수 있는 Solution spaces는 국제공통 평가기준을 활용하여 4장에서 보안요구사항을 도출한다.

3.6.1 Threat Tree 작성

Threat Tree는 DFD의 각 요소에 대한 위협별

상세 정보를 확인하기 위해 트리 형태로 작성한다. LINDDUN 공식 사이트에는 개인정보 위협 트리 카탈로그와 예시를 제공해 주기 때문에 해당 내용을 참고할 수 있다. Table 10,11은 도출된 모든 위협트리 중 Entity와 Data Store의 일부를 나타내었다. Entity는 암호화 미실시, 과도한 데이터를 통한 정보노출, 취약한 패스워드와 토큰정보를 사용할 때 데이터 유출이 발상 할 수 있음을 확인 할 수 있었고 Data store의 경우 서버 자체에서 오류메시지, 구성의 실수, 민감한 정보가 공개 될 때 정보가 유출되는 것을 확인 하였다.

Table 10. Entity Threat Tree

Linkability			
1	L_e		
And	1.1	L_e1 : Data flow or Data Store not fully protected	
	OR	1.1.1	L_e3 : (*) information Disclosure of data store
	OR	1.1.2	L_e4 : Do not encrypt
And	1.2	L_e2 : Excessive PII Information Link	
	OR	1.2.1	L_e5 : Information based on IP address and MAC address
	OR	1.2.2	L_e6 : Game play information and service-based information
	OR	1.2.3	L_e7 : Information based on ID, name, friend list, message history
	OR	1.2.4	L_e8 : Information based on photos, music, and home video content
	OR	1.2.5	L_e9 : Information based on Date of birth, nationality, language used
Identifiability			
1	I_e	I_e1 : Login using identifiable information	
	1.1	I_e2 : Use the identity itself for membership	
	OR	1.1.1	I_e5 : Use I-PIN
	OR	1.1.2	I_e6 : Use mobile phone number
	OR	1.1.3	I_e7 : Use email address
And	1.2	I_e3 : Knowledge-based login	
	OR	1.2.1	I_e8 : Login with weak password
	OR	1.2.2	I_e9 : Data store is vulnerable
And	1.3	I_e4 : Login with vulnerable token information	
	OR	1.3.1	I_e10 : When the maximum scope of authority is required
	OR	1.3.2	I_e11 : Requested read and write permission
	OR	1.3.3	I_e12 : Do not store client credentials and tokens on the back-end server
	OR	1.3.4	I_e13 : When the refresh token is not used

Table 11. Data Store Threat Tree

Identifiability			
1	I_DS		
And	1.1	I_ds1 : Data access control vulnerability	
	OR	1.1.1	I_ds3 : (*) Information Disclosure of data store
And	1.2	I_ds2 : Anonymization of vulnerable data	
	OR	1.2.1	I_ds4 : (*) Identifiability of entity
	OR	1.2.2	I_ds5 : User identification through data inference and re-authentication
Detectability			
1	D_DS		
And	1.1	D_ds1 : Data access control vulnerability	
	OR	1.1.1	D_ds3 : (*) information Disclosure of data store
And	1.2	D_ds2 : Weak information hiding	
Disclosure of information			
1	ID_DS		
And	1.1	ID_ds1 : (*) information disclosure of STRIDE Threat Modeling	
And	1.2	ID_ds2 : Directory Indexing	
	OR	1.2.1	ID_ds7 : The directory index is allowed.
	OR	1.2.2	ID_ds8 : The Web server is configured incorrectly.
And	1.3	ID_ds3 : Information Leakage	
	OR	1.3.1	ID_ds9 : Exploits a web site that reveals sensitive data such as error data
	OR	1.3.2	ID_ds10 : sensitive information, comments, error messages, if the source code exists

And	1.4	ID_ds5 : Path Traversal	
	OR	1.4.1	ID_ds11 : Access to files outside the root directory
And	1.5	ID_ds6 : bypass protection measures	
	OR	1.5.1	ID_ds12 : No data store protection measures
	OR	1.5.2	ID_ds13 : Easy to obtain authorization
	OR	1.5.3	ID_ds14 : Unencrypted

3.6.2 MUC 작성

MUC(Misuse Case)는 Threat Tree를 통해 도출된 위협이 실제 환경에 적용되는 시나리오를 작성해 이해를 높이기 위해 문서화한다. MUC에는 식별자, 요약, 주요 공격자, 공격의 흐름과 결과를 작성한다. Table 12는 3.6.1에서 도출한 Threat Tree에 대한 일부 MUC를 나타내었다.

IV. 보안기능 요구사항 도출

본 장에서는 STRIDE, LINDDUN 위협모델링을 통해 식별된 잠재적 위협을 국제공통평가기준을 활용하여 보안요구사항을 도출한다. 4.1절에서 가정 사항, 위협, 조직의 보안정책을 통해 보안의 특성과 범위를 나타내고 4.2절에서 알려진 위협에 대응할 수 있는 보안목적을 정의한다. 마지막으로 4.3절에서 보안목적을 만족시키기 위한 보안요구사항을 도출한다.

4.1 TOE 보안환경

TOE 보안환경은 보안특성과 범위를 정의하기 위해 가정 사항, 위협, 운영환경을 작성한다. 4.3절에서 도출하는 보안목적에 모든 보안환경이 만족함을 보이기 위해 각각의 항목에 번호를 부여하였다.

Table 12. Misuse Case of Entity and Data store

MUC	Specification		
MUC 01	Threat Tree	Linkability_Entity	
	Summary	Users upload their game data to social network services and the attacker collects their personal profile through related information	
	mis-actor	skilled outsider	
	Basic path	bf1	The game user uploads the ranking results to the social network service linked with the game ID
		bf2	The attacker can check the related conversation in the game message store with insufficient confidentiality
		bf3	Continue to view message content and uploads from photos, video files, and social accounts
	Consequence	Identify personal information based on messages that are less confidential and files uploaded to social accounts	
MUC	Specification		
MUC 02	Threat Tree	Identifiability_Entity	
	Summary	Obtain credentials that are not stored securely and pretend to be legitimate users	
	mis-actor	skilled outsider	
	Basic path	bf1	Attacker gets information during login process with weak password
		bf2	Performs the synchronization process between the game account and the console account.
		bf3	Obtain an access token as a client credential that is not stored securely on the back-end server
	Consequence	Ability to steal unauthorized credentials and impersonate a user	
Omitted			

4.1.1 가정 사항

가정 사항은 TOE가 안전하게 운영되고 범위와 경계를 다루기 위해 작성된다. 또한 사용목적, 운영환경, 역할과 책임 항목에 대해 요구사항 개발에 필요한 필수적 환경조건 및 현실적 문제를 포함하여 작성한다. 아래 하위 절은 각 항목에 대한 설명을 나타내었다.

(1) 사용목적 및 역할

A1. STRONG_CRYPTO : 암호알고리즘은 데이터를 보호하기에 충분히 견고하다.

A2. FAIR_USE : 수집되고 생성되는 데이터는 오직 인가된 목적을 위해 사용되어야 한다.

(2) 운영환경

A3. PHYSICAL_PROTECTION : TOE 서비스를 제공하는 네트워크 장비는 물리적 공격에 대응수단을 갖추고 있으며 이를 전제로 안전하게 운영 한다.

A4. CREDENTIALS_SECURE : TOE에 필요한 하드웨어, 소프트웨어, 펌웨어는 알려진 취약점에 대해 정기적으로 업데이트 및 관리 한다.

(3) 인적 역할 및 책임

A5. ACCESS_NOTICE : 사용제한, 서비스 수준에 관련된 정보를 사용자에게 명확히 명시 한다.

A6. TRUSTED_ADMIN : TOE에 관련된 관리자는 보안지침을 준수하여 운영한다.

4.1.2 위협

STRIDE와 LINDDUN의 위협트리에서 도출한 세부 위협을 유사 위협끼리 분류하기 위해 작성된다. 본 논문은 NIAP(National Information Assurance Partnership)에서 TOE에 유사하게 사용되는 네트워크 장비, 무선랜 접근시스템, 암호시스템 등 공인된 PP를 선정 하여 위협을 정의하였고 차이가 있는 부분은 추가적으로 새롭게 도출 하였다. 위협에 대한 결과는 Table 13에 정리 하였다.

4.2 보안목적

보안목적은 위협의 발생을 방지하고 해결하기 위한 명확한 설명을 제공한다. TOE와 TOE운영환경을 방지, 탐지, 정정을 고려하여 보안환경에서 식별된 가정

Table 13. Threat in TOE security Environment

NO	Threat	Description	Tree Node	
T1	T.UNAUTHORIZED_ACCESS	The threat agent bypass security functions during authentication and communication.	AT	1.1.1, 4.1, 4.2
			TT	I_ds2, D_ds1, I_p, NR_p2, ID_p, D_df
T2	T.PRIVLEGED_USER_ERROR	Authorized users bypass security functions or install unauthorized software.	AT	4.2
			TT	U_e, NR_df
T3	T.SECURITY_FUNCTION_COMPROMISE	The threat agent can access the device through unauthorized software.	AT	1.3.1, 3.1.1, 3.1.2, 3.2.1
			TT	N/A
T4	SPOOFING_ATTACK	A threat agent may act improperly as a spoofing subject.	AT	1.2.4
			TT	L_e1, I_e4, L_ds1, NR_ds1, NR_P1,
T5	T.PASSWORD_CRACKING	The threat agent can access the device by exploiting the vulnerability of the authentication process.	AT	1.1, 1.2, 1.3, 1.4
			TT	I_e1, I_e3, I_e4, I_ds1
T6	T.INTERNAL_THREAT	Threats by careless insiders and inappropriate policies	AT	1.1.4, 1.2.6
			TT	L_e2, U_e1, L_ds2,ID_ds, NC_ds, NC_p
T7	T.NETWORK_ATTACK	A threat agent may access and tamper with data transmitted over the network.	AT	2.1.1
			TT	I_ds1, NR_ds3,ID_ds, NR_p3, ID_df
T8	RESOURCE_ATTACK	Consumes extensive resources through human error, software, and hardware.	AT	3.1.1, 3.1.2
			TT	N/A

사항과 위협에 대응하고 운영환경을 강화하기 위한 방법을 서술한다. 아래에는 4.1절에서 도출한 보안환경에 대응하는 결과를 나타내었다.

O1. PROTECTED_STORAGE : 데이터 저장소의 무단 접근에 대응하기 위해 데이터 기반 보호를 사용 한다.

O2. TRUSTED_CHANNEL : 수동적, 능동적 네트워크 공격을 해결하기 위해 중요데이터는 신뢰할 수 있는 채널을 통해 전송 한다.

O3. TRUST_FAULT : 부적절한 행위로 인해 장애가 발생한 경우에도 서비스를 유지한다.

O4. AUDIT_GENERATION : 부적절한 매크로 및 악의적 행동을 통해 서비스를 방해하는 사용자, 공격자를 추적할 수 있도록 기록하고 경고를 발생시킨다.

O5. AUDIT_PROTECT : 인가되지 않은 변경, 삭제에 대한 감사 기록을 보호하여 사용자의 책임성을 보장한다.

O6. SELF_CONFIRM : 펌웨어, 소프트웨어는 허가되지 않은 데이터 변경으로부터 보호해야 한다.

O7. SECURITY_TRANS_DATA : TOE를 통해 생성 및 저장되는 데이터의 기밀성을 제공한다.

O8. TOKEN_MANAGEMENT : 인증에 사용되는 키와 토큰은 안전하게 생성, 분배되며 인가되지 않은 접근 및 변경으로부터 보호된다.

O9. DOS_PROTECT : 서비스 공격에 대응하기 위해 전체 자원소비를 유동적으로 조절한다.

OE1. MEDIATE : 조직의 보안정책에 따라 사용자 데이터를 보호한다.

OE2. TRUSTED_ADMIN : 서비스에 관련된 모든 관리자는 적절히 훈련되고 명확한 정책을 준수하여 관리 및 운영한다.

OE3. DISPLAY_BANNER : 조직은 TOE 사용에 관한 권고 및 경고사항을 명확하게 명시한다.

4.3 보안기능 요구사항 및 완전성 검증

4.2절에서 도출한 보안목적을 만족하기 위해 보안기능요구사항을 작성한다. 본 논문에서는 6개의 가정사항, 8개의 위협을 파악하였고 각 항목이 12개의 보안목적에 모두 부합함을 확인하였다. 각 보안목적은 최소한 하나의 보안기능요구사항으로부터 추적이 가능함을 보임으로서 완전성을 확인할 수 있었다. Table 14는 해당 결과를 나타낸다.

Table 14. Security Functional Requirements and Mapping

NO	Element	NO	Object	Functional Components	
T1	UNAUTHORIZED_ACCESS	O2	TRUSTED_CHANNEL	FDP_IFC.2	Complete information flow control
				FDP_IFF.1	Simple security attributes
				FMT_MSA.3	Static attribute initialisation
				FMT_MSA.1	Management of security attributes
				FMT_SMR.1	Security roles
				FMT_SMF.1	Specification of Management Functions
				FIA_UID.1	Timing of identification
				FTP_ITC.1	Inter-TSF trusted channel
				FIA_UAU.1	Timing of authentication
		O7	SECURITY_TRANS_DATA	FDP_UCT.1	Basic data exchange confidentiality
				FTP_TRP.1	Trusted path
T2	PRIVLEGED_USER_ERROR	O4	AUDIT_GENERATION	FAU_ARP.1	Security alarms
				FAU_SAA.1	Potential violation analysis

				FAU_GEN.1	Audit data generation
				FPT_STM.1	Reliable time stamps
				FAU_SAA.2	Profile based anomaly detection
				FIA_UID.1	Timing of identification
				FAU_SAA.4	Complex attack heuristics
		O5	AUDIT_PROTECT	FAU_SAR.1	Audit review
				FAU_GEN.1	Audit data generation
				FPT_STM.1	Reliable time stamps
				FAU_SAR.2	Restricted audit review
				FAU_STG.4	Prevention of audit data loss
				FAU_STG.1	Protected audit trail storage
Omitted					
T5	PASSWORD_CRACKING	O2	TRUSTED_CHANNEL	FDP_IFC.2	Complete information flow control
				FDP_IFF.1	Simple security attributes
				FMT_MSA.3	Static attribute initialisation
				FMT_MSA.1	Management of security attributes
				FMT_SMR.1	Security roles
				FMT_SMF.1	Specification of Management Functions
				FIA_UID.1	Timing of identification
				FTP_ITC.1	Inter-TSF confidentiality during transmission
				FTP_TRP.1	Trusted path
		O8	TOKEN_MANAGEMENT	FTA_SSL.1	TSF-initiated session locking
				FIA_UAU.1	Timing of authentication
				FIA_UID.1	Timing of identification
				FTA_SSL.2	User-initiated locking
				FTA_SSL.3	TSF-initiated termination
				FTA_SSL.4	User-initiated termination
				FTA_LSA.1	Limitation on scope of selectable attributes
				FIA_AFL.1	Authentication failure handling
				FIA_SOS.1	Verification of secrets
				FIA_SOS.2	TSF Generation of secrets
				FIA_UAU.2	User authentication before any action
				FIA_UAU.3	Unforgeable authentication

T6	INTERNAL_ THREAT	O7	SECURITY_TRANS_DATA	FDP_ETC.2	Export of user data with security attributes
				FDP_IFC.1	Subset information flow control
				FDP_IFF.1	Simple security attributes
				FMT_MSA.3	Static attribute initialisation
				FMT_MSA.1	Management of security attributes
				FMT_SMR.1	Security roles
				FMT_SMF.1	Specification of Management Functions
				FMT_MOF.1	Management of security functions behaviour
				FIA_UID.1	Timing of identification
				FMT_MSA.2	Secure security attributes
				FMT_MSA.4	Security attribute value inheritance
				FMT_MTD.1	Management of TSF data
				FMT_MTD.3	Secure TSF data
Omitted					

V. 결론 및 향후 과제

서로 다른 플랫폼 플레이어들이 동일 게임 콘텐츠를 플랫폼에 상관없이 언제 어디서든 함께 즐길 수 있는 크로스플레이가 지원되면서 게임시장은 더욱 성장하고 있다.

이에 본 논문은 콘솔 게임의 보안 관련 연구를 살펴보고 Serverless computing에서 사용자의 숙련도와 기타 요소를 고려하여 유연한 매칭을 제공하는 크로스플레이 환경을 STRIDE와 LINDDUN 모델링을 활용하여 위협을 도출하였다. 또한 국제공통평가기준을 활용하여 크로스플레이에 대한 보안요구사항을 도출하여 분석범위의 완전성과 추적성이 만족함을 보였다. 본 연구를 통해 도출된 위협과 보안요구사항은 향후 서비스를 지원하는 게임회사에서 참고할 수 있을 것으로 예상한다.

하지만 본 논문은 콘솔사용자와 Session기반 멀티플레이 게임으로 범위를 제한하였기 때문에 추후 전체 플랫폼으로 범위를 넓혀서 분석하는 연구가 필요하다. 또한 크로스플레이는 현재 도입되는 단계이며 키보드와 마우스로 컨트롤 가능한 PC사용자들의 일방적인 게임진행 그리고 제조사별 추구하는 비즈니스 방향의 차이로 제한되는 사항 역시 우선적으로 해결해야할 과제로 남아있다.

References

[1] Newzoo, "Global_Game_Market_Report," [Internet], https://resources.newzoo.com/hubfs/Reports/Newzoo_Global_Games_Market_Report_2017.

[2] Gameple, "Platform Border Game," [Internet], http://www.gameple.co.kr/news/articleView.html?idxno=142867.

[3] Microsoft, "The STRIDE Threat Model," [Internet], https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v%3dcs.20)

[4] Denis Verdon, "Risk Analysis in Software Design," IEEE Security&Privacy, vol. 2, No. 04, pp.79-84, July. 2004.

[5] NIST, "Risk management guide for information technology systems," [Internet], http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[6] C.S.E.institute," OCTAVE," [Internet], http://www.cert.org/octave/

[7] UcedaVelez, "Real World Threat Modeling using the PASTA Methodology," in

Proceedings of OWASP AppSec Research 2012.
〔8〕 Brenda Larcom, "Trike," 〔Internet〕, http://www.octotrike.org/
〔9〕 LINDDUN "A privacy threat analysis framework," 〔Internet〕, https://linddun.org/
〔10〕 Privacy Office, Office of Information Technology, "PRIVACY IMPACT ASSESSMENT (PIA) GUIDE",Revised January 2007.
〔11〕 NymityInc, 〔Internet〕, https://www.nymity.com/
〔12〕 Johnny Chung lee, "Hacking the Nintendo Will Remote," IEEE Pervasive Computing, vol. 7, No. 3 pp:39-45, August 2008.
〔13〕 Arunasalam Sambhanthan, "Microsoft's Kinect Technology: A Bust That Could Still Become a Boom," IEEE Consumer Electronics Magazine, Vol. 7, Issue 3, pp.99-101, April 2018.
〔14〕 Jeff Yan and Brian Randell, "An Investigation of Cheating in Online Games," IEEE Security & Privacy, vol. 7, Issue: 3, pp.37-44, June 2009.
〔15〕 Jason Moore, Ibrahim Baggili, Andrew Marrington and Armindo, "Preliminary Forensic Analysis Of The Xbox One", DIGITAL FORENSIC RESEARCH CONFERENCE, pp.57-65, August 2014.
〔16〕 Francois Mouton, Mercia M, Louise Leenen and H.S Venter, "Social Engineering Attack Framework," IEEE 2014 Information Security for South Africa, pp. 1-9, Nov. 2014.
〔17〕 Grobauer, B, "Understanding cloud computing vulnerabilities," IEEE Security & Privacy, pp. 50 - 57, June. 2010.
〔18〕 ChiragMod, Dhiren Patel and Bhavesh Borisaniya, "A survey of intrusion detection techniques in cloud," vol. 36, pp. 42-57, January 2013.
〔19〕 Hanqian Wu, Yi Ding, Chuck Winer and Li Yao, "Network security for virtual machine in cloud computing," IEEE Conference on Computer Sciences and Convergence Information Technology, pp.18 - 21, Nov. 2010.
〔20〕 Aaqib Iqbal Wani, "A Survey of Security Issues and Attacks in Cloud and their Possible Defenses," IJETER Vol. 5, Issue 12, December 2017.
〔21〕 LuisRodero-Merino, "Building safe PaaS clouds: A survey on security in multi tenant software platforms," Computers & Security, Vol 31, pp. 96-108, February 2012.
〔22〕 Jeff Yan and Brian Randell, "An Investigation of Cheating in Online Games," IEEE Security & Privacy, vol. 7, pp. 37-44, May. 2009.
〔23〕 Stephen Mohr and Syed Shawon Rahman, "IT Security Issues Within the Video Game Industry," Cryptography and Security, pp. 16, Nov. 2011.
〔24〕 Prandini, "Splitting the HTTPS stream to attack secure web connections," IEEE Securiry & Privacy, vol. 8, pp. 80 - 84, Nov. 2010
〔25〕 Collin jackson, "ForceHTTPS: protecting high-security web sites from network attacks," 17th International Conference on WWW, pp. 525-534, April. 2008
〔26〕 Marin silic, Jakov Krolo and goran Delac, "Security vulnerabilities in modern web browser architecture," IEEE, MIPRO, 2010 Proceedings of the 33rd International Convention, May. 2010.
〔27〕 Michael McIntosh, "XML signature element wrapping attacks and countermeasures," 2005 workshop on Secure web services, pp. 20-27, Nov. 2005.
〔28〕 A. Kieyzun, P. J. Guo, K. Jayaraman, and M. D. Ernst. "Automatic creation of SQL injection and cross-site scripting attacks", IEEE, pp. 16-24, May. 2009.

[29] Chonka, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," vol. 34, pp. 1097-1107, July 2011.
[30] Thangavel, Nithya S and Sindhuja R, "DoS Attacks Over Cloud Environment: A Literature Survey," in Advancing Cloud Database Systems 2017, IGI Global. pp. 289-319
[31] Zhifeng Xiao and Yang Xiao "Security and privacy in cloud computing," IEEE Communications Surveys, vol. 15, pp. 843 - 859, July. 2012.
[32] Duncan, "An overview of insider attacks in cloud computing. Concurrency and Computation," CCPE, Experience, vol. 27, March. 2014
[33] Lee S, Kim Y, and Kim J, "Stealing web pages rendered on your browser by exploiting GPU vulnerabilities," In IEEE symposium on security and privacy, pp 19 - 33, May. 2014.
[34] Zhou Z, Diao W, Liu X, Li Z, Zhang K, Liu R, "Vulnerable GPU memory management: towards recovering raw data from GPU," Proc Privacy Enhancing Technol, vol. 2017, pp. 57 - 73, Apr. 2017.
[35] Nancy Arya, "Hypervisor Security - A Major Concern," International Journal of Information and Computation Technology," vol. 3 pp. 57 - 73, Nov. 2013.
[36] G. Pek, L. Buttyan, and B. Bencsath, "A survey of security issues in hardware virtualization," ACM Computing Surveys, vol. 45, pp. 1 - 34, Nov. 2013.
[37] Dorottya Papp, Zhendong Ma and Levente Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," IEEE Conferences in PST, pp. 145 - 152, July. 2015.
[38] Ang Cui, Michael Costello and Salvatore J. Stolfo, "When Firmware Modifications Attack: A Case Study of Embedded exploitation," Published 2013 in NDSS, May. 2016.
[39] Kyung-Soo Lim and Sangjin Lee, "A Methodology for Forensic Analysis of Embedded Systems," 2008 Second International Conference on Future Generation Communication and Networking, vol. 2, pp. 283 - 286, Nov. 2008.
[40] Daniel Fett, Ralf Kuesters and Guido Schmitz "A Comprehensive Formal Security Analysis of OAuth 2.0," CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Aug. 2016.
[41] Marios Argyriou, "Security Flows in OAuth 2.0 Framework: A Case Study," SAFECOMP 2017: Computer Safety, Reliability, and Security, pp 396-406, Sep. 2017.
[42] Roman Unuchek, "Leaking Ads—Is User Data Truly Secure?," RSA Conference, April. 2018.
[43] Marlinspike, "M.: New tricks for defeating SSL in practice," BlackHat-DC-09, Apr.2013
[44] Liu, H, "A new form of DoS attack in a cloud and its avoidance mechanism," ACM Workshop on Cloud Computing Security, pp. 65 - 76, October. 2010
[45] Wu H, Ding Y, Winer C and Yao, L, "Network security for virtual machine in cloud computing," IEEE 5th International Conference on Computer Sciences and Convergence Information Technology, pp. 18 - 21, February. 2010.
[46] Joe Bialek, Microsoft OSR, "A Dive into Hyper-V Architecture & Vulnerabilities.", Black Hat 2018.
[47] Jordan Rabet, Microsoft OSR, "Hardening Hyper-V through Offensive Security Research," Black Hat 2018.
[48] Mark McGloin and Phil Hunt, "OAuth 2.0 Threat Model and Security Considerations," RFC6819, January 2013.

[49] Common Vulnerabilities and Exposures, "CVE-2018-8491," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8491
[50] Common Vulnerabilities and Exposures, "CVE-2018-8470," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8470
[51] Common Vulnerabilities and Exposures, "CVE-2018-8357," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8357
[52] Common Vulnerabilities and Exposures, "CVE-2018-5178," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5178
[53] Common Vulnerabilities and Exposures, "CVE-2018-8493," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8493
[54] Common Vulnerabilities and Exposures, "CVE-2018-15121," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15121
[55] Common Vulnerabilities and Exposures, "CVE-2018-0957," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0957
[56] Common Vulnerabilities and Exposures, "CVE-2018-8489," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8489
[57] Common Vulnerabilities and Exposures, "CVE-2018-8438," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8438
[58] Common Vulnerabilities and Exposures, "CVE-2018-8495," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8495
[59] Common Vulnerabilities and Exposures, "CVE-2018-8492," [Internet], https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8492
[60] hyp3rlinx, "Microsoft Internet Explorer 11.371.16299.0 (Windows 10) - Denial Of Service," Exploit Database, 2018-04-24
[61] Common Criteria Recognition Arrangement, "Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model," Ver3.1, CCMB-2017-04-001, 2017
[62] Common Criteria Recognition Arrangement, "Common Criteria for Information Technology Security Evaluation Part 2 : Security functional components," Ver3.1, CCMB-2017-04-002, 2017
[63] Common Criteria Recognition Arrangement, "Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components," Ver3.1, CCMB-2017-04-003, 2017

〈저자소개〉

김 동 우 (Dong-Woo Kim) 학생회원
2015년 2월: 울산대학교 전기공학부 컴퓨터정보통신 졸업
2017년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 보안공학, 보안성 평가, 금융보안

강 수 영 (Soo-young Kang) 학생회원
2006년 2월: 순천향대학교 컴퓨터공학부 공학사
2008년 2월: 순천향대학교 컴퓨터공학부 공학석사
2008년 5월~2010년 10월: 한국인터넷진흥원(KISA) 연구원
2010년 10월~2014년 10월: 안랩(Ahnlab) 주임연구원
2013년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 보안성 평가/인증, 위협 모델링, 소프트웨어 보안

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2017년~현재: 고려대학교 사이버무기시험평가연구센터(CW-TEC) 부센터장
2004년~현재: 한국정보보호학회 이사
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: (사)화이트해커연합 HARU 및 국제해킹대회 SECUINSIDE 설립자 및 이사
2012년: 선관위 디도스 특별검사팀 자문위원
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현재: 방위사업청 방산기술보호 자문관
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 국방보안연구소 정보보호분야 자문위원
2017년~현재: 여신금융협회 신용카드 단말기 시험 인증위원회 위원
〈관심분야〉 보안공학 및 SDL, 위협 리스크 모델링, 보안성 평가/인증, 암호학, Usable Security